AU/ACSC/2016

AIR COMMAND AND STAFF COLLEGE
AIR UNIVERSITY

COMBATING TERRORISM:
NORTH AMERICAN AEROSPACE DEFENSE COMMAND VERSUS ASYMMETRIC THREATS

by
Joseph W. Stevens, Maj, USAF

A Research Report Submitted to the Faculty
In Partial Fulfillment of the Graduation Requirements

Proposal Advisor: Dr. Steve R. Schwalbe
Project Advisor: Dr. Gregory F. Intoccia

Maxwell Air Force Base, Alabama
February 2016

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

TABLE OF CONTENTS

ACKNOWLEDGMENTS

I would like to thank the staff of instructors at the Air University who mentored me through this online master's program, especially Dr. Intoccia for guiding my research project and providing a generous amount of recommendations, patience, and encouragement. Additionally, a special thanks to all my fellow classmates for their honest feedback and engaging topics. Also, thank you to my senior leaders, supervisors, and co-workers at the Eastern Air Defense Sector for sharing their insight and for professionally executing the homeland defense mission.

Finally, I give the most sincere thanks to family for their unconditional love and support. Specifically, my gorgeous and loving wife, who inspires me to excel at everything I do, sacrifices unselfishly to allow me to accomplish goals, and teaches me what is most important in life. Also, I want to thank my beautiful and brilliant daughter, for her love, compassion, and perpetual blessing, as well as, her noble husband, for his laughter, knowledge, and service to this country.

LIST OF ILLUSTRATIONS

ABSTRACT

This paper's purpose determines what changes will better enable the North American Aerospace Defense Command (NORAD) to deter, detect, and defeat low radar cross-section (RCS) technologies targeting U.S. citizens and U.S. infrastructure. Despite NORAD changes since September 11, 2001, evidence shows low RCS technologies are still penetrating their airspace. Consequently, this paper employs the problem solution methodology to discern NORAD vulnerabilities. In addition, the paper explores possible U.S. policies and U.S. intelligences organizational changes that would better support NORAD in defending the homeland.

The paper's key findings deduce that sensor settings are not optimized to detect low RCS technologies. Additionally, NORAD is not the lead government agency managing airspace or aerial domestic terrorism within its area of responsibility. Also, certain U.S. policies restrict military forces during homeland defense operations because of legal penalty and jurisdiction barriers. Moreover, intelligence organizations are keeping secrets from one another and not sharing data efficiently.

This paper's key recommendations include designing an operational toggle switch for NORAD and the Federal Aviation Administration to quickly manage sensor thresholds and mission displays. Furthermore, Posse Comitatus Act amendments allowing NORAD forces to legally operate during domestic aerial attacks. Finally, intelligence organizations collect data via social media sources too.

SECTION I: INTRODUCTION

We the People of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defense, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Prosperity.

- United States Constitution

Strategically, the United States (U.S.) government has no greater responsibility than protecting the American people.[1] In order to sustain state sovereignty, it is essential to effectively employ the four national instruments of power: diplomacy, informational, military, and economic. Since 1957, the North American Aerospace Defense Command (NORAD) has been the military component entrusted with executing the nation's top priority of preventing catastrophic attacks on the U.S. homeland or critical infrastructure.[2]

Initially, the NORAD mission focused on the ability to detect, deter, and defeat aerial symmetric threats. Since 2009, NORAD reports successfully intercepting 50 Russian aircraft nearing its border.[3] However, on September 11, 2001 (9/11) NORAD vulnerabilities were exposed when terrorists hijacked four commercial aircraft to conduct aerial attacks within the United States killing 2,977 people.[4] Despite NORAD constructing an interior radar network system and implementing Operation Noble Eagle (ONE) to counter subsequent asymmetric attacks, a gyrocopter flew 80 miles on April 15, 2015, through restricted airspace and landed on the Capitol lawn, thus indicating that NORAD remains vulnerable.

Specifically, low radar cross-section (RCS) aircraft, which are generally smaller than the single-engine propeller Cessna, present significant technical challenges for the current NORAD radar network system to detect, which in turn makes defeating any threat involving low RCS technology a potential national security concern.[5] As a result, intelligence agencies fear that terrorist organizations could be planning to attack the United States using low RCS aircraft like a gyrocopter, remotely piloted aircraft system (RPAS) and Club-K cruise missile (CM) to perpetuate an attack while evading detection.[6] In fact, the Federal Bureau of Investigations (FBI) thwarted a plot in September 2011 targeting the Pentagon and U.S. Capitol using RPAS filled with C-4 explosives.[7] Even though low RCS aircraft have a reduced range and payload capability, their yield for death and destruction across the full range of conventional, biological, radiological, nuclear and explosive (CBRNE) is of vital importance and demands attention.

Consequently, this paper will explore the following question: What changes will enable NORAD to better detect and defeat aerial asymmetric threats targeting U.S. citizens and U.S. infrastructure in the event deterrence fails and a terrorist attacks using low RCS technologies?

In order to detect and defeat asymmetrical threats targeting U.S. citizens and U.S. infrastructure by using low RCS technologies, NORAD must adjust or develop sensors for detection to defeat aerial threats in the event deterrence fails. Also, U.S. policies and intelligence agencies influencing counterterrorism efforts must facilitate the NORAD mission and not inhibit its objectives.

First, this research argues that if NORAD does not make drastic changes on detecting low RCS technologies, then their tactical ability to defeat any asymmetric terrorist attack is moot, since current counterair engagements require sensor cueing to prevent fratricide and minimize collateral damage. Any aerial aircraft capable of releasing CBRNE agents is a major concern to NORAD, but combating this threat without the ability to detect is illogical when serving the highest priority to protect national security, U.S. citizens or infrastructure.

Second, this paper argues that if U.S. does not adapt strategy and change federal laws that will assist NORAD defenses, then achieving an end state to the Global War on Terrorism

(GWOT) within the homeland is futile. Specifically, updating the Posse Comitatus Act (PCA) to allow military forces to conduct necessary actions without legal penalty is crucial for NORAD success. NORAD interacts with several joint partners to perform homeland defense, but legally does not have the same freedoms as other government agencies to combat domestic asymmetric threats. Also, combatant command (COCOM) apportionments are alarming, based on the homeland defense being the top priority, yet advanced U.S. weapon systems are deployed overseas.

Third, this paper argues that intelligence is the first line of defense in counterterrorism, but it is not maximizing its capabilities to assist NORAD. For example, intelligence detection capabilities are able to fill NORAD vulnerable gaps. Also, the gross bureaucratic framework of federal, state, and local intelligence agencies creates jurisdiction and data flow barriers that are not conducive to time-sensitive targets associating asymmetric threats.

The framework for this research applies the problem solution methodology to determine what changes NORAD needs to make to be able to effectively deter, detect, and defeat aerial asymmetric threats targeting U.S. citizens and U.S. infrastructure, if terrorists attack using low RCS technologies. Section II provides the reader background on NORAD operations before and after 9/11, as well as the current U.S. policies codified to counterterrorism. Next, Section III examines how NORAD plans to deter, detect, and defeat low RCS threats. Section IV discerns how U.S. policies are facilitating and inhibiting NORAD operations. Section V explores how intelligence agency functions can better assist NORAD in combating terrorist using low RCS technologies.

Finally, Section VI summarizes the paper's key arguments involving NORAD detection, U.S. policy facilitations, and U.S. intelligence organization functions supporting counterterrorism. Also, it provides unbiased recommendations for NORAD and its joint partners to consider changing to conduct offensive counterair operations against the emerging asymmetrical threats using low RCS technologies. Moreover, it implores that U.S. decision makers should not ignore the empirical evidence on how terrorists plan to employ low RCS aircraft with CBRNE agents, which undermines the NORAD mission. Lastly, in spite of military drawdowns and declining resources, this paper will clarify options on how NORAD and its integral parts can best combat terrorism, which is currently threatening the premise of the Constitution in securing national sovereignty.

SECTION II: BACKGROUND

This section highlights pertinent facts that are relevant to the research analysis sections. First, data focuses on the North American Aerospace Defense Command (NORAD) operations before and after the events of September 11, 2001 (9/11). Next, material covers the current United States (U.S.) policies and laws in use to combat terrorism. Finally, it provides information detailing intelligence organization counterterrorism functions. Collectively, they are some of the main factors allowing low radar cross-section (RCS) threats to occur.

NORAD Pre-9/11

The origin of NORAD dates back to 1957, when the United States and Canada formed a bi-national alliance to defend against the Soviet long-range bombers and atomic threats.[8] Since the Atlantic and Pacific oceans could no longer provide a comfortable national shield, NORAD devised a three-tiered radar network made up of 90 ground-based and maritime sensors that provided Strategic Air Command (SAC) two hours warning for an aerial interdiction response.[9] Initially, these early warning sensors were strategically positioned along the coastline and oriented outward to detect inbound symmetric aircraft (figure 1).[10] The SAC strategy during this period was nuclear deterrence.

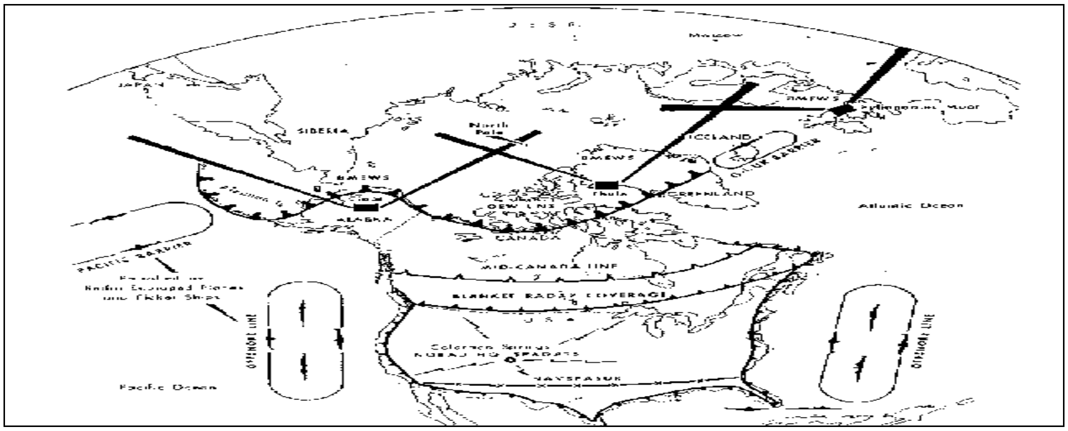


Figure 1: NORAD Radars in the 1960s[11]

Based on the emergence of space assets during the 1960s and 1970s, NORAD reconfigured its radar network system to include ground, airborne, and space sensors for detection against Soviet intercontinental and sea-launched ballistic missile threats.[12] Offensively, SAC developed a nuclear triad consisting of bombers, submarine-launched ballistic missiles (SLCMs), and intercontinental ballistic missiles (ICBMS). Defensively, SAC received early warning detection signals from the "Iron Triad" that was comprised of the E-3, E-8, and RC-135, respectively. Furthermore, hardened combat command centers were constructed in Colorado Springs, Colorado (i.e. Cheyenne Mountain) and North Bay Ontario to provide command and control (C2) for some 300 interceptors and 100 radars, which costs about $1 billion dollars per year.[13]

Prior to September 11, 2001, the tension between the United States and the Soviets reached its peak on October 22, 1962 during the Cuban Missile Crisis. Amid this 13-day period, NORAD was placed on defense readiness condition (DEFCON) 2 for the first time in history, in response to a deployment of Soviet ballistic missiles to Cuba.[14] Nonetheless, the crisis ended with the help of diplomatic agreements, which became a common trend during the Cold War preventing NORAD and the Soviets from ever engaging in direct conflict.

Following the Cold War, the economy and the perception of an unlikely threat prompted a congressional mandate forcing NORAD to make major changes, hence reducing its homeland defense posture. For instance, the NORAD alert air defense force allocations drastically went from 180 aircraft down to 20.[15] In addition, tactical control authority of the NORAD air sovereignty mission was now the responsibility of the Air National Guard, operating from four different air defense sectors within the continental United States (CONUS). The ground-based radar systems remained along the perimeter of the coastline to maintain vigilance on any approaching symmetric threats, as well as simultaneously adding a new focus on counter drug operations. To date, NORAD has arguably succeeded in its ability to detect and deter symmetric threats, but as of 9/11 the same could not be said in regard to asymmetric threats.

NORAD Post-9/11

On 9/11 when terrorists hijacked four civilian aircraft, the United States suffered the most devastating attack within its sovereign border. Specifically, terrorists targeted U.S infrastructure striking the Pentagon in Washington D.C. and the World Trade Center in New York City. Amid this horrific chain of events, NORAD experienced difficulties managing basic C2 functions.[16] Two key contributing factors restraining the NORAD response in providing protection on 9/11 were alert resources and radar coverage.[17]

Regarding resources, the CONUS NORAD Region (CONR) had an apportionment of 14 alert fighters available to defend the CONUS on the morning of 9/11, compared to the 26 alerts sites during the Cold War (figure 2).[18] This disparity came from perceptions of a Soviet threat reduction and economic downsizing. Analytically, the flux of forces overseas to Europe and Korea suggests that decision makers prefer engaging Russia, if needed, over their soil instead of the United States. Also, the appropriation of assets to combatant commanders (COCOMs) fighting conflicts abroad was a key contributor.[19] Nonetheless, the C2 operator not seeing a target is arguably one of the most salient factors inhibiting NORAD from defeating aerial threats.

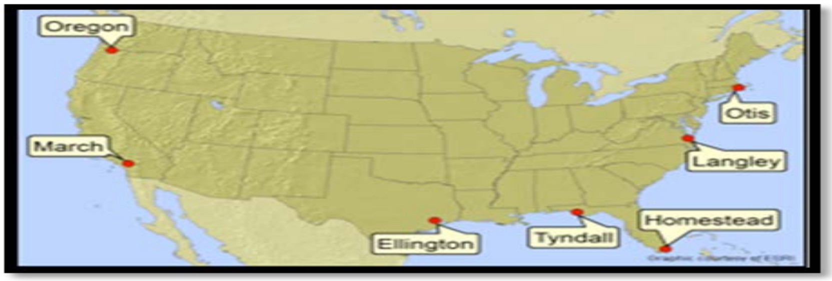


Figure 2: CONUS Alert Sites on 9/11[20]

During the events of 9/11, the NORAD radar network system did not have sufficient sensor coverage within the interior of the CONUS, since long range radars were strategically placed on the coast to extend early warning detection of inbound symmetric threats (figure 3). The only interior radar coverage came from the Federal Aviation Administration (FAA) ARS-9 radars, which were located near significant airfields. Although, NORAD does gain situational awareness by launching an Airborne Warning and Control Systems (AWACS) or other Iron Triad platforms to the vicinity of a hijacked aircraft, but it requires time and proper coordination. Specifically, the Federal Bureau of Investigations (FBI) handles counterterrorism and the Federal Emergency Management Agency (FEMA) is the lead for resolving the situation, hence NORAD merely facilitates support due to the Posse Comitatus Act (PCA).[21]

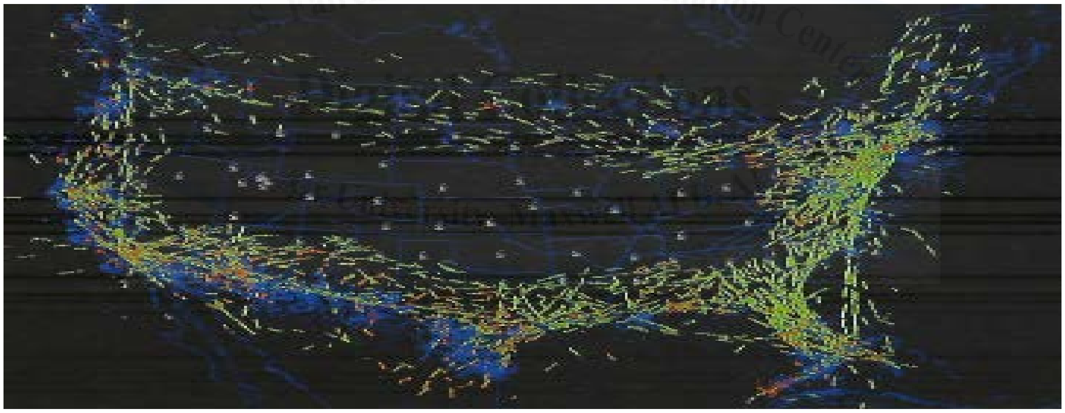


Figure 3: NORAD Pre-9/11 Radar Picture[22]

Following the tragic events of 9/11, NORAD evolved its mission, restructured its defenses, and adjusted its surveillance focus to detect threats internally and externally. Currently, the two primary missions NORAD supports involve air sovereignty and Operation Noble Eagle. Also, the commander of NORAD (CDRNORAD) became dual-hatted in 2002 when President Bush signed a new Unified Command Plan (UCP) establishing the U.S. Northern Command (USNORTHCOM).[23] The role of this new COCOM is to provide C2 for the

Department of Defense (DOD) homeland defense effort. Also, it coordinates and assists defense support of civil authorities (DSCA) missions, such as domestic emergencies and law enforcement operations.[24] Moreover, USNORTHCOM integrates with 60 federal and non-federal agencies liaisons, including the Department of Homeland Security (DHS).[25]

Nevertheless, the primary mission objectives for NORAD remain unchanged, which are to deter, detect, and defeat all airborne threats (i.e. symmetric and asymmetric). However, NORAD resources have drastically increased. For instance, a congressional budget approved funds to extend the radar sensor network for coverage inside the NORAD area of responsibility (AOR), create a Domestic Events Network (DEN) 24/7 hotline, and double the allocation of alert fighters (figure 4). Still, these additional resources do not stop asymmetric threats that have a low RCS from penetrating NORAD restricted airspace.

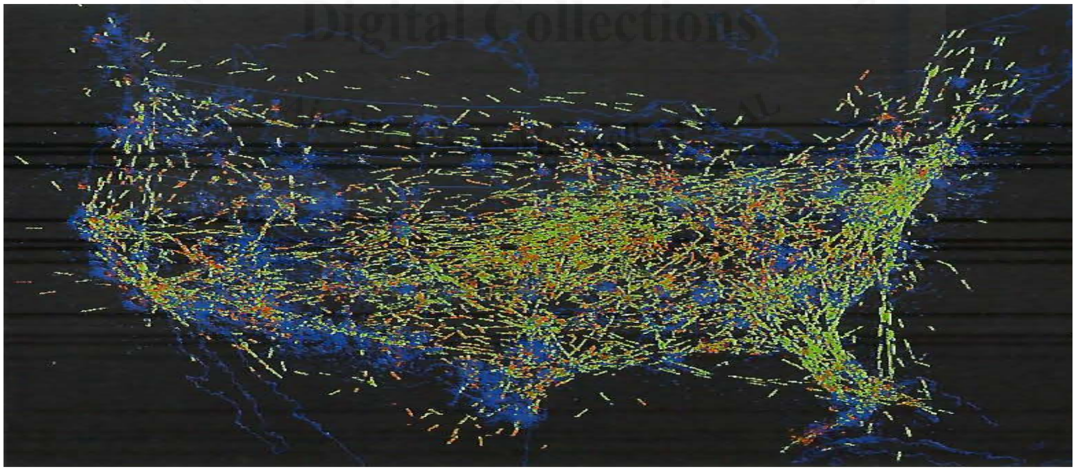


Figure 4: NORAD Radar Picture Post-9/11[26]

For example, a gyrocopter landed on the U.S. Capitol lawn in 2015 and a remotely piloted aircraft system (RPAS) crashed on the Whitehouse lawn in 2016. Moreover, multiple RPAS fly undetected within the NORAD AOR, exposing both vulnerability and flight safety concerns. If these low RCS aircraft are not being properly detected, then the terrorists have aerial means to attack. Since RPAS have crashed near the German Chancellor during a rally and delivered radioactive material to the Japanese Prime Minister's residence, logically this technology could be used by terrorist organizations to target the United States.[27] Therefore, unless NORAD makes changes to its key operational principles, the probability to detect and defeat all threats, especially low RCS aircraft (i.e. gyrocopter, RPAS or Club-K), is doubtful. However, current U.S. policies are exacerbating NORAD abilities to effectively counter asymmetric threats, thus requiring counterterrorism policy changes.

U.S. Policies and Laws Influencing Counterterrorism

Arguably, U.S. policy is strategically the first line of defense against terrorism. Examples of U.S. policies and laws perpetuating and inhibiting counterterrorism are the National Security Strategy (NSS), National Military Strategy (NMS), Patriot Act, and PCA. Additionally, there are many variables that cause terrorism, but it is evident that some terrorists oppose certain Western ideological characteristics, such as capitalism, secularism, and democracy. For instance, U.S. capitalism perpetuates globalization, which is a Western movement to open free markets and international borders, but it undoubtedly acts as a double-edge sword. Globalization concepts create disdain and subsequent motivation for terrorist attacks, but it also offers tools (i.e. internet and transportation) to spread propaganda messages, recruitment, and avenues for attack opportunities.[28] Prior to addressing these factors, it is beneficial to review acts of terrorism that prompt such policies.

The word terrorism comes from the Reign of Terror that Maximilien Robespierre inflicted during the French Revolution to transform the monoarchy into a liberal democracy.[29] Over time, the term terrorism segemented into non-state and international organizations. The latter became prominent in the 1960s and hijacking was its favored tactic.[30] In 1961, the first aircraft hijackings occurred in the United States, prompting President Kennedy to amend the Federal Aviation Act of 1958, thus making it a crime to hijack an aircraft.[31]

In 1977, the Omnibus Antiterroism Act sought to strenghten Federal programs and policies for combating international and domestic terrorism, especially regarding aircraft security.[32] Furthermore, it was instrumental in defining roles and regulations for hijacked aircraft. In June 1995, the Department of Justice was deemed the lead agency via the FBI for terrorist incidents that involved hijacked aircraft over United States juristiction, not the FAA.[33]

Gloablly, the International Civil Aviation Organization (ICAO) is the governing body for flight safety that meets annually at the Convention on International Civil Aviation (Chicago Convention) and publishes documents on civil aviation rules and regualtions.[34] Chicago Convention, Article 1 recognizes that "Every State has complete and exclusive sovereignty over the airspace above its territory."[35] Nevertheless, in 1984, the Chicago Convention amended Article 3 mandating that "States are to refrain from resorting to the use of weapons against civil aircraft in flight."[36] This rule was modified following the events of Septemer 11, 2001, when terrorists used hijacked aircraft as weapons, thus sparking asymmetric threat defense concerns. Clearly, NORAD and U.S. policy changes happen in a reactionary manner. Still, changes in intelligence agency supporting functions are just as vital to the NORAD deter, detect, and defeat objective amid subsequent attacks on the U.S. homeland.

U.S. Intelligence Organization Counterterrorism Functions

If U.S. policy is strategically the first line of defense in counterterrorism, then intelligence organizations, which support NORAD operations, are tactically the first line of defense. Intelligence operates in three primary areas: the collection and interpretation (i.e.

analysis) of information; the protection of government secrets against hostile intelligence services and other threats (i.e. counterintelligence); and the clandestine manipulation of events in foreign lands on behalf of a nation's interests, through the use of propaganda, political activities, economic disruption, and paramilitary operations.[37] Each area is equally important and intrinsically connected to the other. Moreover, all areas are useful in complementing NORAD functions, but focus will only cover collection and interpretation.

Intelligence collection comes from a variety of sources. For example, technical intelligence (TECHINT) via satellites and intelligence, surveillance, and reconnaisance (ISR) platforms, human intelligence (HUMINT) from espionage, and open-source intelligence (OSINT), which is putting together facts by sifting through information available in open literature.[38] Signals intelligence (SIGINT) captures communications from one person to another using a combination of communications intelligence (COMINT) and electronic intelligence (ELINT).[39]

Measurement and signature intelligence (MASINT) is capable of identifying gases emitted from factories specific to weapon systems and locating underground weapons of mass destruction or conventional weapons caches.[40] Finally, geospatial intelligence (GEOINT) collects via satellites, aircraft, and RPAS, which are very expensive, but there are also key conduits for its dissemination of intelligence data.[41] Before its dissemination, intelligence data goes through an analysis phase via a six part joint intelligence process.[42]

The head of all joint intelligence partners is the Director of National Intelligence (DNI), who is a principle advisor to the President and leads 17 intelligence organziations (figure 5).[43] The DNI has 10 function mission support activities, which includes the national counterrorism center (NCTC) serving as the primary organization for analyzing intelligence pertaining to terrorism. However, domestic terrorism is the exception, since it is the responsibility of DHS.[44]

Collectively, their timely and actionable intelligence is the most critical enabler to protecting the homeland, thus the NORAD mission.[45] The next sections provide analysis focusing on NORAD, U.S. policy, and intelligence agency interactions to deter, detect, and defeat aerial threats employing low RCS technologies.

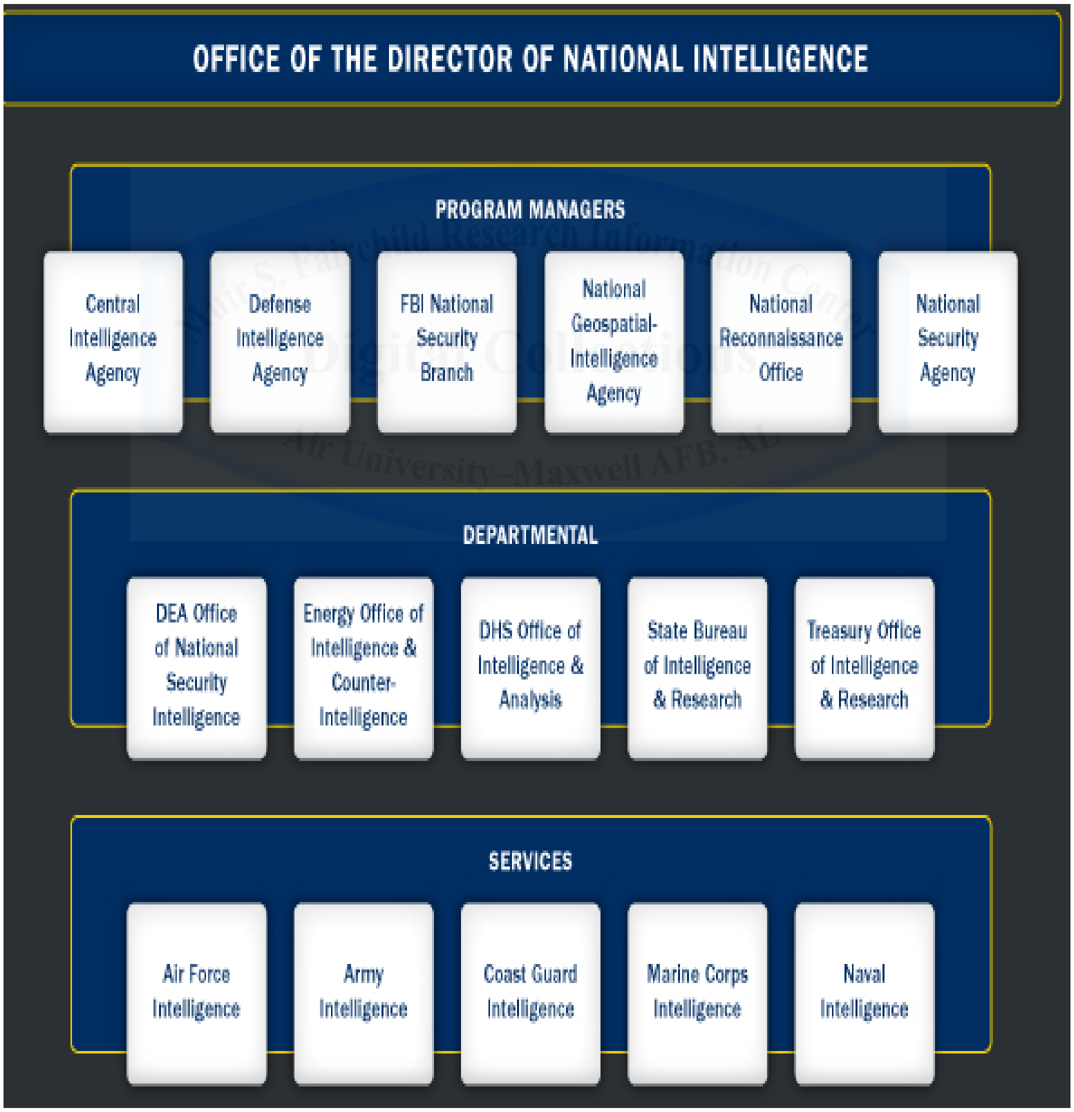

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
PROGRAM MANAGERS
Central Intelligence Agency
Defense Intelligence Agency
FBI National Security Branch
National Geospatial-Intelligence Agency
National Reconnaissance Office
National Security Agency
DEPARTMENTAL
DEA Office of National Security Intelligence
Energy Office of Intelligence & Counter-Intelligence
DHS Office of Intelligence & Analysis
State Bureau of Intelligence & Research
Treasury Office of Intelligence & Research
SERVICES
Air Force Intelligence
Army Intelligence
Coast Guard Intelligence
Marine Corps Intelligence
Naval Intelligence

Figure 5: The U.S. Intelligence Community[46]

SECTION III: NORAD OBJECTIVES

Since the enemy lives in the seams, we are seeking a new level of understanding and efficiency among the Geographic Combatant Commands (GCCs) in order to deter, detect and, when necessary, defeat threats before they pose a danger to the homeland.

- Adm William Gortney

Even though NORAD has seen many changes over the course of its 59-year history, its mission to provide aerospace warning, aerospace control, and maritime warning in the defense of North America has not.[47] The NORAD threat spectrum ranges from symmetric annihilation (i.e. nuclear), DSCA (natural disasters), counter drug operations, and asymmetric activity (terrorism). Since the probability of thermonuclear war is low and the Global War on Terrorism (GWOT) is an ongoing mission, the NORAD focus is currently on asymmetric defense.[48] However, the recent gyrocopter landing, multiple RPAS incidents, and pending Club-K threat reveal gaps within the NORAD objectives. The fact that low RCS technologies are still penetrating the NORAD AOR without being defeated warrants change, which starts by measuring the objectives: deter, detect, and defeat.

Deter

Nuclear deterrence has been a central element of U.S. security policy since the atomic bombings of Hiroshima and Nagasaki in 1945. Psychologically, this deterrence concept premises on preventing action by fear of the consequence, thus persuades a potential adversary that the risk and cost of their actions far outweigh any gains that might be achieved.[49] Moreover, to strengthen deterrence efforts and gain credibility, the U.S. instruments of power (IOP) synergistically work together to serve the common goal of protecting national sovereignty. However, NORAD, the military component of the IOP for homeland defense, is arguably a product and victim of various diplomatic, economic, and informational factors that impacts the deterrence objective.

Diplomatically, NORAD is the product of a bi-national alliance between the United States and Canada that formed to deter a Soviet nuclear attack. Nevertheless, diplomatic failures often result in war or acts of aggression, which is debatably why non-state actors who oppose diplomatic globalization are currently targeting the U.S. homeland with asymmetric tactics.[50] Furthermore, non-state actors (i.e. terrorist organizations) do not exercise sovereignty over any given state and typically seek to undermine state credibility by attacking their ability to govern, deterrence is not as effective.[51] Moreover, U.S. retaliation adds extra layers of diplomatic challenges, which makes targeting internationally cumbersome. Domestically, the multiple jurisdictions encompassing NORAD functions during an asymmetric engagement are equally cumbersome.

Ideally, deterrence is dependent on developing effective policies well in advance of an adversary's attempt to alter the status quo. This requires decision makers to devise a tailored strategy and policy, effectively communicate objectives, and respond to potential threats well in advance of any adversary taking action. Since the United States prefers to fight aggressors as far from the homeland as possible, it ultimately has negative impacts for NORAD operations.[52]

For instance, there is a potential fallacy that U.S. forces fighting abroad distances threats, thus reducing the anxiety and risk perceptions of the American populace. However, deployed U.S. forces supporting political agendas (i.e. alliances, containment, and globalization) arguably fuel terrorist organization desires to attack the U.S. homeland.[53] Also, the flux of COCOM apportionments overseas leaves NORAD with a nominal defense force operating previous generation weapon systems to protect an AOR over 7.6 million square miles. Economically, the

2013 downsizing of two 24-hour NORAD alert facilities perhaps reduces the deterrence of symmetric and asymmetric adversaries seeking potential gaps to exploit.[54] Despite these diplomatic and economic examples, NORAD has informational factors that are vitally impacting its deterrence functions too.

Since NORAD is a C2 headquarters for three regional air operation centers (AOC) in Alaska, Canada, and CONUS, their continuous integration via the informational IOP component is paramount (figure 6). Theoretically, NORAD and USNORTHCOM strengthen its deterrence posture by associating with over 60 federal, state, and local agencies serving the homeland defense (HD) mission. However, terrorist organizations are actively seeking relatively inexpensive tactics of infiltrating cyberspace networks, thus disrupting NORAD communications and aerial defense capabilities that function to deter, detect, and defeat threats.[55] The cyberspace domain also makes retaliation difficult, based on intrinsic universal characteristics that cross many state borders.

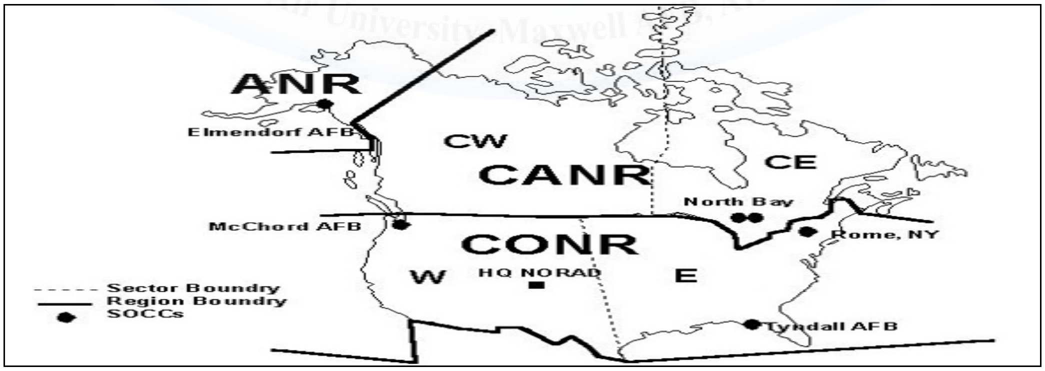


Figure 6: NORAD Area of Responsibility[56]

Analytically, the deterrence spectrum is deducible to three parts: dissuasion, denial, and threat. First, dissuasion is the most passive method which influences via public opinion, diplomacy, and propaganda, but does not incorporate violence or punitive action.[57] Second, the denial method (i.e. no fly lists) reduces the probability for success and forces aggressors to accept added risk.[58] Third, the threat method incorporates punitive measures through diplomatic and economic sanctions, but its credibility is undermined if not implemented.[59] Each part is a function through counterterrorism (CT) and antiterrorism (AT) organizations that ultimately coincide and impact NORAD and other IOP objectives.

In contrast to passive methods of deterrence, (i.e. public opinion, diplomacy, and propaganda), active methods of deterrence (i.e. no fly zones and airport screening) exist. A prime example of active deterrence within the National Capital Region (NCR) is the FAA Notice to Airmen (NOTAM) 6/2069, dated 9 February 2016, prohibiting RPAS weighing less than 55 pounds from flying within the flight restricted zone (FRZ).[60] The FRZ is roughly a 15 nautical mile radius around the Ronald Reagan Washington National Airport (DCA) from surface to 18,000 feet (figure 7).[61] This legislation supports the NORAD effort in combating targets in close proximity to a priority resource. Still, terrorists do not follow rules and take risks; therefore United States credibility via enforcements remains to be seen.

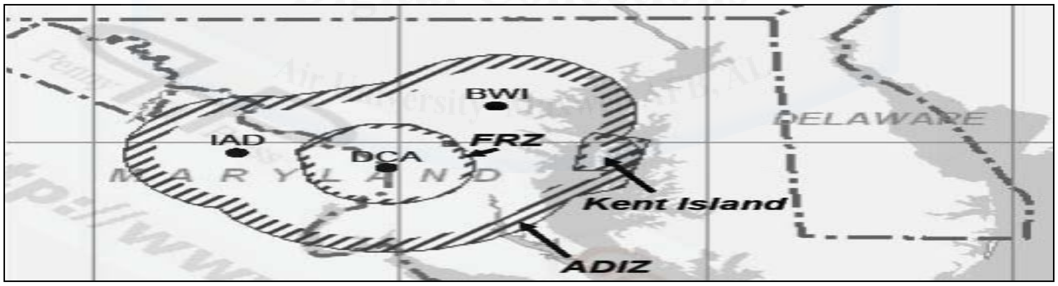


Figure 7: National Capital Region Airspace Restrictions[62]

All in all, for NORAD to successfully achieve its objective to deter asymmetric threats, it must effectively work in concert with the diplomatic, economic, and informational national powers, as well as specialized CT partners. Nevertheless, not only do these rogue regimes and non-state actors pose significant threats to U.S. interests, but their tactics consisting of terrorism, cyberspace attacks, and low RCS employment are among the more difficult to deter.[63] The latter is even more challenging, since the NORAD ability to deter exponentially diminishes without having an ability to detect.

Detect

The Unified Command Plan tasks each combatant commander with, detecting, deterring, and preventing attacks against the United States, its territories and bases, and employing appropriate force to defend the nation should deterrence fail.

- JP 3-01

Defensively, NORAD comprises joint forces from two countries, integrates with global partners, and operates a myriad of early warning systems to perform a counterair mission for HD. Originally, the NORAD radar network consisted of 33 ground-based radars known as the Pinetree Line. Subsequently, early warning system designs evolved producing the Distant Early Warning Line (DEW Line), Over-the-Horizon Backscatter (OTH-B), ballistic missile early warning (BMEWS), and Phased Array Warning System (PAVE PAWS). Today, the NORAD radar network relies on Air Route Surveillance Radars (ARSR), maritime assets, air, space, and cyber assets, Tethered Aerostat Radar System (TARS), and the Joint Land Attack Cruise Missile Defense Elevated Netted Sensor System (JLENS) for its aerial threat detection capability.

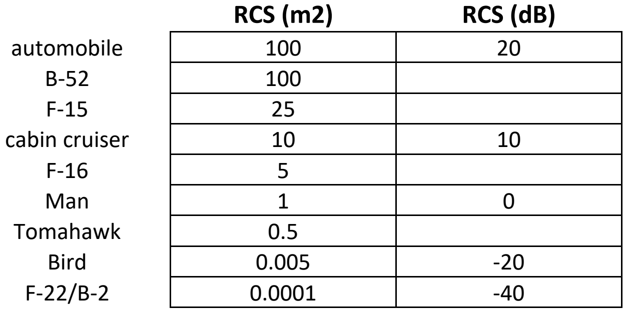
Still, low RCS technologies (i.e. RPAS, gyrocopters, and CMs) are continuing to prove to be elusive targets that are difficult to detect, despite their years of existence.[64] Specifically, the first ever CM, the German V1, took flight in 1944.[65] Nonetheless, the United States has relied on a nuclear deterrence strategy that terrorist organizations are currently undermining, thus threatening national security. To counter another asymmetric attack, NORAD needs to optimize radar filter settings, modify its layered detection capabilities, and develop new detection technologies, as needed.

Since NORAD integrates with some FAA radars, they are subjected to sifting through over 200,000 civil aircraft that fly in excess of 24 million flight hours on an annual basis.[66] This results in saturating the NORAD operator's air picture functions for processing manual detection and potential tracking of aerial threats, thus leading to operational filtering.[67] Furthermore, these radars are susceptible to radar limitations (i.e. terrain masking and range resolution), jamming, and weather anomalies (i.e. trapping, sub-refraction, and super-refraction). Moreover, the radar returns a NORAD operator sees stems from computer program algorithms on what is deemed good and bad data. Collectively, machine function and analysis needs NORAD attention to resolve missing or misinterpreting potential asymmetric aerial threats with low RCS.

If filters are opened, then NORAD operators must process all radar returns displayed, which is challenging and prone to error. However, HD is strategically deemed a “no fail” mission, thus needs to doctrinally maximize contingency plans via redundancy (i.e. layers of defense).[68] Since low RCS asymmetric threats typically fly at low altitudes, there are various COAs to enhance detection capabilities (i.e. airborne assets, computer tracking, and radars targeting a specific parameter).

The AWACS is a proven detection asset, but it is a low density/high demand aircraft, an expensive alternative, and is not under constant operational control (OPCON) of CDRNORAD during peacetime rules of engagement (ROE). Also, AWACS have intensive maintenance and repair records that frequently make them unable to fly, plus they have limited on-station mission times.[69] Therefore, ground-based sensors are the more fiscal and reliable option.

Ground-based sensors have a wide range of capabilities and their settings can detect aerial objects measuring a -20db RCS (figure 8).[70] Nevertheless, this sensitivity is deemed counterproductive for day-to-day operations, since it jeopardizes the FAA’s primary focus of providing flight safety for larger RCS (i.e. ≥ 5 m2) aircraft needing control guidance. Moreover, low RCS detection capabilities do exist in some sensors, but they are not being utilized.[71] Unless there are detection changes involving radar filters, defense layering, and new sensor technology development, NORAD is taking risks on missing asymmetric threats using low RCS aircraft.



	RCS (m2)	RCS (dB)
automobile	100	20
B-52	100	
F-15	25	
cabin cruiser	10	10
F-16	5	
Man	1	0
Tomahawk	0.5	
Bird	0.005	-20
F-22/B-2	0.0001	-40

Figure 8: Radar Cross-Section Comparisons[72]

Another factor warranting change is the way NORAD conducts their real-world mission while simultaneously conducting training via a live-over-simulation mode. For instance, the Air Defense Sector (ADS) was in the middle of conducting exercises when authorities called for assistance during 9/11, prompting "Is this real-world or exercise?" ambiguity.[73] Typically, DOD units conduct training separate from real-world events, then deploy for mission execution. However, NORAD systems currently do not have this luxury, with the exception of specialized simulations (i.e. Virtual Flag), therefore conduct training scenarios during real-world events. Statistically, the combination of conducting real-world and training missions simultaneously increases errors, impacts detection focus, and better enables low RCS to penetrate the NORAD AOR.

Despite COCOM apportionments, radar limitations, and operational procedures, the NORAD mission to detect all aerial objects remains. Innovative technology (i.e. Advanced Refractive Effects Prediction System) might help, but it is not a fiscal guarantee.[74] Therefore, NORAD presently does not utilize a viable detection capability for low RCS technologies, thus the kill chain process to find, fix, track, target, engage, and assess (F2T2EA) is degraded. Consequently, the NORAD objective to defeat aerial asymmetric threats is a major concern, since radar sensor cueing helps minimize fratricide and collateral damage.

Defeat

Since deterrence is not an absolute, NORAD air defenses, such as alert fighters and the NCR-Air Defense System (NCR-IADS), are inherently the last line of defense in defeating an aerial threat that penetrates its AOR. Moreover, if NORAD detects a terrorist organization attack using low RCS technologies, the window to engage is usually time-sensitive. Nonetheless, U.S. policy defining jurisdiction of authority within its borders is convoluted and handcuffed in bureaucracy. For example, there are standing rules of engagement (SROE) for joint fires outside the United States, but internally the SROE does not apply, unless otherwise directed by the Secretary of Defense (OSD).[75] Furthermore, policy dictating authority to other government agencies (i.e. FBI and FAA) only delays engagements.

The FBI is the lead agency for suppressing asymmetric threats within the United States, but it does not have the forces or weapons systems to neutralize aerial threats compared to NORAD. This contradicts joint doctrine principles stating that plan, task, and control is normally the responsibility of the command with the preponderance of assets.[76] Undoubtedly, PCA is an integral part of appointing the FBI legal authority. Additionally, DHS, who delegates authority to the FBI, technically has the largest civilian government air force in the world, as well as oversight of United States Coast Guard (USCG) assets.[77] Still, NORAD trains to execute this mission and stands ready to accomplish it, despite not having next generation weapon systems in their arsenal like other COCOMs. If the FBI requires NORAD assistance, military assets must coordinate clearance with the FAA.

The FAA controls all airspace within the United States and is responsible for managing flight safety for civilian and military aircraft.[78] NAV CANADA is the FAA equivalent in Canadian airspace. If NORAD scrambles alert fighters to intercept a track of interest (i.e.

asymmetric target), U.S. pilots must comply with FAA headings, speeds, and altitudes. However, if the mission dictates, NORAD can exercise authority to trump FAA guidance to ensure mission accomplishment by declaring Authorization for Interceptor Operations (AFIO).[79] During these events pilots might accept Military Authority Assumes Responsibility for Safe Separation of Aircraft (MARSA) conditions and immediately terminate AFIO after completing their intercept.[80]

U.S. fighters are not given unlimited access to the airspace within its own borders. Granted, pilots do have the option to operate under visual flight rules (VFR), if weather permitting and they comply with set parameters (i.e. code, communications, altitude, and location). Also, the FAA generates flight restrictions via NOTAM, which all aviators must adhere to during flight. For example, NOTAM 0/8326 is a temporary flight restriction for special security reasons within the NCR from the surface up to, but not including 18,000 feet, which is the restricted airspace the gyrocopter violated on April 15, 2015.[81] A gyrocopter is just one example of a low RCS aircraft that terrorist organizations might employ to fly undetected through the NCR-IADS when attacking a vital U.S. center of gravity (COG).

In an effort to protect our political and military leadership, the NCR-IADS was developed following the events of 9/11 (figure 9). Doctrinally, it is a classic example of layered defense and contains the essential components to execute F2T2EA (i.e. kill chain) procedures. Sequentially, the process starts with radars detecting (i.e. find) a target of interest. Overlapping radar coverage and/or airborne sensors triangulate the radar returns to pinpoint a location (i.e. fix). Next, barring obstruction or anomalies, NORAD operators will monitor its flight path via radar returns (i.e. track). Simultaneously, radio transmissions and visual warning sensors alert aircraft when they violate restricted area procedures, thus demanding pilots make FAA contact or exit the restricted area immediately. Targeting starts once the tactical decision is made to scramble alert aircraft.

Within the NCR, there is a combination of fixed wing and rotary wing assets to conduct intercepts (i.e. target). Airborne interceptors conduct multiple missions, like deterring the target with warning shots or forcing the target to change heading, thus maneuver away from the protected COG. If unsuccessful, the engagement authority (EA) starts actively coordinating all options via a Defense Red Switch Network (DRSN) conference. If the EA gives an order to engage, the pilots employ air-to-air missiles on the target (i.e. engage). Finally, alert aircraft are capable of providing airborne reconnaissance and battle damage assessments (i.e. assess), fuel permitting.

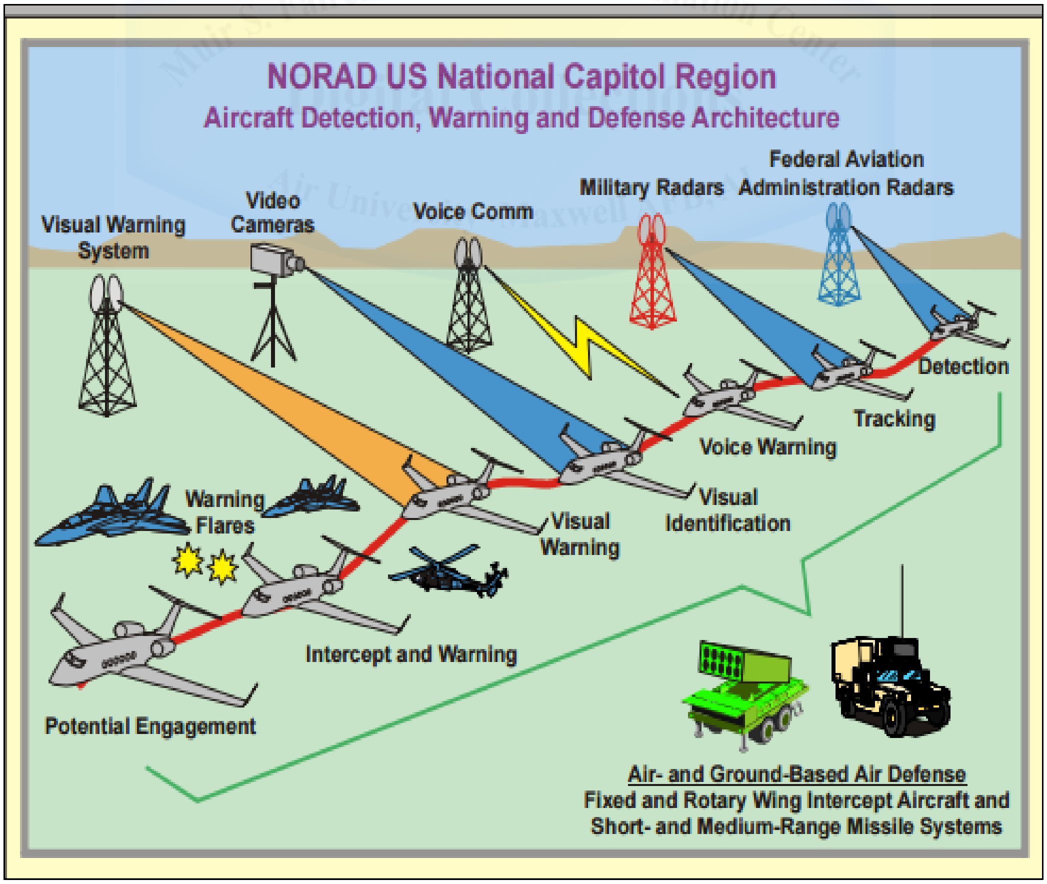

NORAD US National Capitol Region
Aircraft Detection, Warning and Defense Architecture
Visual Warning System
Video Cameras
Voice Comm
Military Radars
Federal Aviation Administration Radars
Detection
Tracking
Voice Warning
Visual Identification
Visual Warning
Warning Flares
Intercept and Warning
Potential Engagement
Air- and Ground-Based Air Defense
Fixed and Rotary Wing Intercept Aircraft and
Short- and Medium-Range Missile Systems

Figure 9: National Capital Region Integrated Air Defense System[82]

Overall, a layered defense provides redundant sensors and multiple engagement opportunities to increase the probability of mission success. To combat a CM threat (i.e. Club-K), NORAD coordinates for OPCON of AWACS, tankers, and fighters to form a long range detection team (LRDT). Subsequently, NORAD integrates with available maritime assets and all other supporting agencies to tactically position assets to deter, detect, and defeat threats. Since NORAD relies and integrates with multiple agencies 24/7, its ultimate objective should be maximizing unity of effort for effective joint interoperability.

In summary, NORAD will not stop the low RCS technology threat alone, nor will it stop aerial asymmetric attacks without significant external changes (i.e. unity of effort) within U.S. policy and intelligence agencies that impact its objectives. Since active and passive deterrence is questionable against an adversary willing to sacrifice themselves (i.e. kamikaze or suicide bomber), detection is perhaps the most vital since it directly impacts defeating threats. Areas that NORAD needs to focus on are filter settings, radar layering, and new technology to remedy sensor detection. Finally, defeating asymmetric threats requires correcting interagency barriers among federal, state, and local partners, which requires changes within U.S. policy. The next section focuses on U.S. policies and laws influencing terrorism.

SECTION IV: U.S. POLICIES AND LAWS INFLUENCING TERRORISM

Since terrorism is the willingness to use violence to affect politics, it is a major concern for any sovereign nation.

- Michael L. Madigan

Since U.S. policy is an integral part of combating terrorist threats, this section focuses on key documents that perpetuate and inhibit counterterrorism efforts, such as the NSS, NMS, Patriot Act, and PCA. Specifically, this section examines U.S. policies and laws that facilitate and impede NORAD functions in performing homeland defense. Furthermore, this section shows how the Constitution, which is the primary document for civilian and military law, guides the NSS and NMS in combating asymmetric threats, thus having residual legal and binding effects on NORAD operations.

National Security Strategy

U.S. policy on countering terrorism was documented by President Reagan in 1987 with the first NSS, in compliance with the Goldwater-Nichols Act of 1987. By law, the NSS is disseminated by the President annually to integrate the IOP and direct the strategic goals of the nation. Since 1987, every U.S. president has reiterated the significance of terrorism within the NSS, since it undeniably threatens national interests. However, in the 2002 NSS President Bush references the GWOT, differentiating it from any other war in history that will be fought on many fronts for an extended period of time.[83] In addition, the NSS clarifies that "To make terrorism – is to delegitimate terrorism, is to make terrorism like genocide, the slave trade or piracy – the kinds of activities that no one who aspires to respectability can condone, let alone support."[84]

Additionally, President Bush published the National Strategy for Counterterrorism in 2003, instilling that protecting and defending the Homeland and the American people remains the first and most solemn obligation, thus the premise of GWOT.[85] In 2013, President Obama perpetuates CT focus with four guiding principles: "adhering to U.S. Core Values; Building Security Partnerships; Applying CT Tools and Capabilities Appropriately; and Building a Culture of Resilience."[86] Collectively, these strategic documents provide the IOP guidance for building interdepartmental strategies, like the National Military Strategy (figure 10).

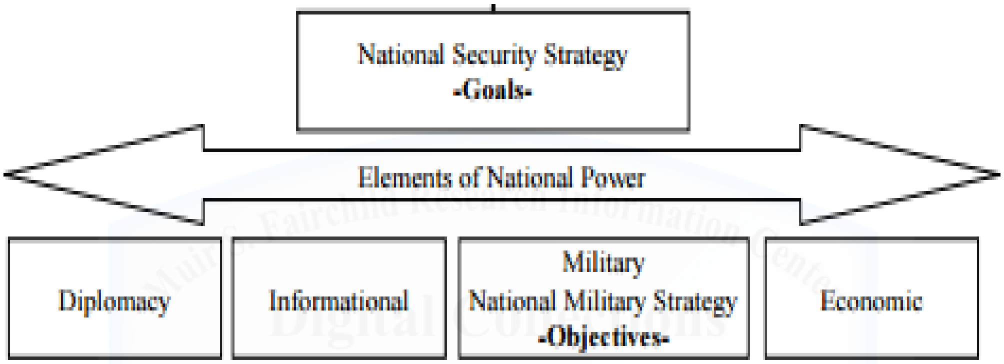

National Security Strategy
-Goals-
Elements of National Power
Diplomacy
Informational
Military
National Military Strategy
-Objectives-
Economic

Figure 10: Strategy Influence on Instruments of Power

National Military Strategy

Per 10 U.S. Code § 153, the NMS is the document drafted by the Chairman of the Joint Chiefs of Staff (CJCS) that provides the OSD the DOD strategy to accomplish the NSS objectives. As a minimum, the NMS outlines and identifies threats, operational concepts, mission priorities, fiscal budgets, force planning, and acquisitions, and challenge assessments affecting NSS goals.[87] Even though maintaining a secure and effective nuclear deterrent is the top priority in the 2015 NMS, it begins with addressing the need to disrupt, degrade, and defeat violent extremist organizations (VEOs).[88]

Since one man's terrorist is arguably another man's freedom fighter, it is important for DOD to define terms. Below are key terms useful in further discussing asymmetric threats.

Terrorism: The unlawful use of violence or threat of violence, often motivated by religious, political, or other ideological beliefs, to instill fear and coerce governments or societies in pursuit of goals that are usually political.[89]

Antiterrorism (AT): Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include rapid containment by local military and civilian forces.[90]

Counterterrorism (CT): Activities and operations taken to neutralize terrorists and their organizations and networks in order to render them incapable of using violence to instill fear and coerce governments or societies to achieve their goals.[91]

Homeland security (HS): A concerted national effort to prevent terrorist attacks within the United States and reduce America's vulnerability to terrorism.[92]

Homeland defense (HD): The protection of United States sovereignty, territory, domestic population, and critical infrastructure against external threats and aggression or other threats as directed by the President.[93]

HD is the primary mission and focus of NORAD and has been for decades. However, HS became the focus of DHS and USNORTHCOM in 2002 stemming from the events of 9/11. Subsequently, NORAD and DHS began sharing accountability for the safety and security of the United States, since CDRNORAD assumed command of USNORTHCOM making it a dual-hatted command billet (figure 11). Since an operation might transition from HD to HS or vice versa, collaboration and extensive integration and synchronization is paramount to prevent ambiguous situations over responsibility and authority.[94]

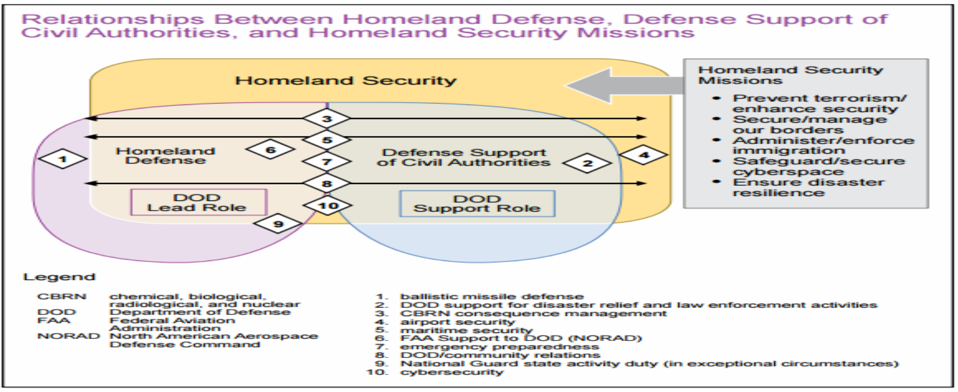

Relationships Between Homeland Defense, Defense Support of Civil Authorities, and Homeland Security Missions
Homeland Security
Homeland Security Missions
• Prevent terrorism/ enhance security
• Secure/manage our borders
• Administer/enforce immigration
• Safeguard/secure cyberspace
• Ensure disaster resilience
Homeland Defense
Defense Support of Civil Authorities
DOD Lead Role
DOD Support Role
1
2
3
4
5
6
7
8
9
10
Legend
CBRN chemical, biological, radiological, and nuclear
DOD Department of Defense
FAA Federal Aviation Administration
NORAD North American Aerospace Defense Command
1. ballistic missile defense
2. DOD support for disaster relief and law enforcement activities
3. CBRN consequence management
4. airport security
5. maritime security
6. FAA Support to DOD (NORAD)
7. emergency preparedness
8. DOD/community relations
9. National Guard state activity duty (in exceptional circumstances)
10. cybersecurity

Figure 11: HS and HD Mission Relationship[95]

Still, the DOD perspective on terrorism remains twofold: antiterrorism and counterterrorism. The antiterrorism policy and responsibilities are detailed in the Department of Defense directive (DODD) 2000.12, DOD Antiterrorism Program, which is overseen by the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD (HD&ASA)).[96] The main function is to operate a 24-hour terrorism intelligence warning and fusion center to ensure that terrorist threat intelligence is timely and accurately disseminated to the appropriate DOD components.[97] The United States Secret Service (USSS) is the primary DHS component that focuses on countering terrorism that threatens American consumers and industry.[98]

The CT policies for DOD are governed by Joint Publication 3-26, which delineates the authoritative roles among U.S. government agencies depending on the threat location. The lead agency for CT within the United States is the DHS.[99] Specifically, the Secretary of Homeland Security is the appointed federal official for domestic incidents management, thus coordinating federal options within the United States to anticipate, prepare for, respond to, and recover from a terrorist attack.[100] Additionally, DHS delegates threats or acts of terrorism that take place within the United States to the FBI.[101] However, "if a terrorist incident exceeds the FBI's capacity, the President may direct DOD to provide domestic CT assistance within Constitutional and statutory limits," within the bounds of the Patriot Act and Posse Comitatus Act.[102]

Patriot Act

The Patriot Act, which is officially known as the Uniting and Strengthening America Act by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, is another residual that came from 9/11. With court approval, the Patriot Act gives federal and state government officials the authority to collect intelligence on U.S. citizens for the purpose of rooting out terrorists to prevent future attacks.[103] Arguably, intelligence is an integral part of being able to detect symmetric or asymmetric threats, which enables the ability to deter and defeat, as long as data flow is efficient.

Since the FBI is lead government agency for counterterrorism within the United States, it is not surprising that they are active in authorizing rights for implementing the Patriot Act. Consequently, the FBI is collecting and sharing information much more effectively than ever before, hence deeming the Patriot Act as the greatest force multiplier in the defense of the nation.[104] Despite the Patriot Act easing intelligence gathering on international and domestic terrorists, certain legal restrictions from the Posse Comitatus Act remain.

Posse Comitatus Act

The PCA of 1878 stems from events following the U.S. Civil War, on the basis of removing federal troops from the South.[105] Nonetheless, PCA creates national controversy and sparks various legal interpretations, but joint doctrine defines it as follows:

> PCA prohibits the use of military personnel from performing various functions within the homeland. However, when directed by the President, the use of military operations for HD is a constitutional exception to the PCA. When performing HD operations, Title 10, United States Code, forces are not subject to the restriction of the PCA.[106]

The basis of PCA is to strengthen civil-military relations by limiting the use of military personnel for law enforcement, but over time exceptions emerged. For example, PCA does not apply when federal troops quell insurrection of presidential power, provide aerial search and surveillance, assist with counterdrug operations, National Guardsmen operate under Title 32, and the USCG operate under Title 14 authority.[107] The USCG assets within the NCR serve USNORTHCOM under Title 14 and NORAD under Title 10. Still, all Title 10 forces must receive orders from the OSD prior to supporting law enforcement officials during an international or domestic terrorism incident within the United States.[108]

In summary, U.S. policies drive subsequent actions that either facilitate or inhibit NORAD efforts against asymmetric threats. The NSS directly impacts the NMS, thus NORAD apportionments. While the Patriot act allows more freedom to investigate potential terrorist activities threatening the homeland, the PCA is still restrictive. Like the Goldwater-Nichols Act prompting joint interoperability within DOD, all government agencies need to have effective integration to maximize unity of effort, especially those serving in homeland defense roles. Namely, PCA changes need to allow military and civilian forces to interact without legal consequences.

Additionally, jurisdiction barriers do not serve the need for time-sensitive action and lead government agency appointments do not match doctrine principles (i.e. control to those with the preponderance of assets). Finally, further research needs to evaluate the benefits of globalization in comparison to the costs associated with GWOT, then determine what other alternatives might exist to better serve the NSS objectives. Such a method would allow the U.S. to spread democratic ideology and increase its capital growth, while simultaneously minimizing the spread and threat of terrorism within the homeland and around the globe. Undoubtedly, the intelligence community is a pivotal actor in this process, thus the focus of the next section.

SECTION V: U.S. INTELLIGENCE ORGANIZATIONS

The collaborative intelligence sharing environment should be capable of generating and moving intelligence, operational information, and orders where needed in the shortest possible time

- JP 3-27

If NORAD is tactically the last line of defense against asymmetric threats, then the intelligence community (IC) is arguably the tactical first line of defense via a supporting role. Joint doctrine states that intelligence preparation of the battlespace (IPB) is an essential element to military operations. Despite the restraints intelligence organizations have sending classified material to federal, state, and local officials, because of security clearance levels and the need to know factor, they are an integral part in defending the homeland against terrorism. In fact, intelligence agency collection methods are effectively proven, thus thwarting terrorist attacks using low RCS technologies. Still, key changes will enable them to be even more effective, especially in the domain of social media. This section will examine the intelligence agency role and their pending assessment about low RCS technology threats.

Joint doctrine states that counterair planning centers on joint intelligence preparation of the operational environment (JIPOE) and IPB, regardless of the threat being symmetric or asymmetric.[109] Intelligence organizations monitoring HUMINT and SIGINT data are potentially the first line of defense in detecting signs of a credible attack. However, intelligence data collection is useless, unless it is a collaborative effort and the information is timely and effectively shared. As a result, the intelligence community relies on the Joint Worldwide Intelligence Communication System (JWICS) to distribute secure information.[110] Still, U.S. classification levels and what is deemed releasable data to joint partners remains a factor, especially for NORAD with Canadian and other global partners.

Conversely, unclassified sources cannot be overlooked in detection efforts either. For example, the gyrocopter pilot that landed on the U.S. Capitol lawn used social media to broadcast his intentions. Subsequently, news media was there waiting; however, the federal, state, and local officials responsible for protecting the area were unaware.[111] NORAD should seek out all possible leads to perform its function to detect, which includes making modifications as necessary. Intelligence organizations are good at keeping secrets, but keeping secrets from one another is not logical. Despite classification levels, the speed at which data moves is essential for time-sensitive targets (i.e. low RCS technologies).

Counterterrorism Functions

To counter low RCS technology targeting the U.S. homeland, the primary weapon in homeland defense is more than likely not going to be an aircraft carrier, or a missile shield. Arguably, the primary weapon is going to be information. Therefore, the homeland defense force needs to be an active and passive network that facilitates the rapid transfer of information domestically and internationally to prevent attacks on the U.S. homeland, citizens, and infrastructure.

Moreover, some might assert that the Homeland Defense Forces should merely be intelligence and computer experts. Regardless of who locates a threat, NORAD has highly capable alert forces ready to eliminate the threat once it is airborne. This is based on its training and Operation Noble Eagle missions. In short, the NORAD problem has not been the ability to destroy the threat, but gaining actionable information prior to the attack. Theoretically, the intelligence method of detection fills the void of ground-based sensor limitations.

Nevertheless, intelligence activities conducted by U.S. intelligence organizations in the United States and its territories are strictly controlled.[112] As previously mentioned, several regulations and laws specifically govern the use of DOD intelligence assets and organizations in domestic operations. In fact, the FBI is the lead government agency on determining what constitutes a National Special Security Event (NSSE), which is an event deemed as a potential target for terrorism or criminal activity (i.e. United Nations General Assembly or Super Bowl).[113] The NSSE is a common terrorist target based on the population and effect it could receive if able to attack. Intelligence agencies consider the RPAS, CM, and gyrocopter as the most probable low RCS technologies for a terrorist to conduct an asymmetric attack.[114]

Perceived Low RCS Threats

Despite the recent gyrocopter landing within the NCR, the RPAS is by far the most prolific low RCS threat on the market. As mentioned, the FBI thwarted a RPAS filled with C-4 explosives from a Massachusetts man wanting to target the Pentagon and U.S. Capitol. Countries abroad (i.e. Germany and Japan) are experiencing RPAS incidents that crash at political events and carry radioactive material. All in all, this threat is real, but preventable with intelligence intervention. The gyrocopter pilot publicized his goal via social media, but the Central Intelligence Agency (CIA), FBI, and other DOD intelligence agencies did not receive this message, unlike the media awaiting the arrival.[115] Social media cannot be overlooked as a possible source of credible intelligence, and circulating information is a collaborative effort in yielding the proper government agency response.

Still, the most lethal low RCS technology is by far the CM, especially the Club-K. The Club-K is a Russian manufactured CM launching system containing four missile tubes, plus its versatility allows it to launch from a variety of land, maritime, truck, and rail platforms.[116] Currently, Iran has purchased a Club-K, but other rogue nations or non-actor states might acquire this weapons system to threaten the United States.[117] Since the Club-K is a low RCS technology and a high speed threat, it compresses the NORAD kill chain response, thus undermining their objectives to deter, detect, and defeat, unless changes occur. This requirement falls on NORAD, U.S. policy and intelligence agencies responsible for defeating this emerging threat of low RCS technologies via asymmetric tactics.

In summary, intelligence organizations are a vital part of defending counterterrorism. In fact, the FBI leads the efforts against domestic terrorism. However, U.S. laws still restrict action (i.e. collection), especially DOD intelligence activities amid domestic operations or against U.S. citizens. Nonetheless, the framework of the intelligence community should be better integrated to streamline the dissemination of data. Their current data posing as low RCS technology threats include the gyrocopter, RPAS, and CM, respectively.

Furthermore, the AT program focuses on the detection and prevention of terrorist attacks against DOD personnel, installations, and infrastructure critical to mission accomplishment, including the planning and preparation to respond to terrorist incidents. Intelligence provides the CDRNORAD with the terrorist group’s operational capability, intentions, and activity, as well as the operating environment within which friendly forces operate. Collectively, these factors make NORAD more effective in defending against low RCS technologies.

SECTION VI: CONCLUSION

Recommendations

Even though there has been an absence of hijacks within the North American Aerospace Defense Command (NORAD) area of responsibility (AOR) since September, 11, 2001 (9/11), intelligence organizations report a new threat is emerging via low radar cross-section (RCS) technologies. Such an attack could release conventional, biological, radiological, nuclear and explosive (CBRNE) agents that would potentially yield a death toll well above 3,000 casualties, create wide spread panic, and jeopardize national security. If NORAD is to effectively perform the homeland defense mission and prevent another 9/11-type asymmetric attack, then correcting known vulnerabilities are an absolute. Based on research findings, this paper suggests seven recommendation areas.

One, NORAD and the Federal Aviation Administration (FAA) share common radars, but the FAA focuses more on flight safety, hence reducing its detection capability of low RCS objects to prevent saturating its operational air picture. This practice creates vulnerability gaps and prevents NORAD from having the most accurate data for defending the homeland. To fix it, NORAD and the FAA can design a switch to allow both agencies to display the data they require to perform their specific missions. Just because the FAA is the lead agency and controls the airspace over the United States should not dictate an authority that undermines national security. Also, NORAD having its own radars, new technology, and layered defense is an advantageous option to prevent conflicts.

Two, the Posse Comitatus Act (PCA) limits military forces from interacting in civil affairs. Since NORAD has a major role in defending the homeland, such legal restrictions are inhibiting the efficiency and effectiveness of the NORAD mission. Despite modifications allowing Title 32 and Title 14 forces to assist civil law enforcement organizations during natural disasters, more changes involving a terrorist crisis are essential. NORAD, who is ultimately responsible and accountable for homeland defense, should not have constraints from a law codified in 1878 when defending a modern threat.

Three, a fundamental function of an intelligence organization is to keep secrets, but keeping secrets from other intelligence organizations is a potential problem. The 9/11 Commission Report found that information sharing was not occurring and procedures were routinely ignored. However, the Goldwater-Nichols Act mandates joint integration amongst DOD forces, so similar legislation could garner results for intelligence organization interactions. Tools exist to disseminate credible data (i.e. the Joint Worldwide Intelligence Communication System), but without passing timely and accurate information, NORAD response times are diminished. This includes intelligence detecting threats via sensors that NORAD is not seeing.

Four, NORAD consoles display training and real-world mission data returns simultaneously, thus creating ambiguity. Fixing this problem via a formal training unit (FTU) requires fiscal dollars to accommodate extra buildings and consoles to fully separate training and real-world operations. Like other command and control assets (i.e. Airborne Warning and Control Systems), NORAD needs training, currency, and proficiency events. However, training separate from real-world events logically prevents distractions and reduces errors.

Five, the gyrocopter pilot’s intentions were available on social media, but intelligence organizations failed to collect it. Local news reporters were aware and waiting, while the agencies responsible for protecting the National Capital Region were not. Acknowledging all open source methods, then validating collection data for credibility, prevents perpetuating this occurrence, NORAD embarrassment, and national security concerns.

Six, NORAD alert bases have downsized since 9/11, thus limiting response times to defeat asymmetric threats. Reduction via complacency from a lack of attacks is not the answer when national security is at risk. Ensuring NORAD has tactical spacing throughout its AOR is paramount, since conducting an intercept against a time-sensitive target requires alert asset proximity to be viable. Moreover, providing proper detection with sufficient assets available to defeat threats will strengthen deterrence, thus a more proactive posture in comparison to the trend of a reactionary increase following attacks.

Seven, deterrence diminishes by allowing gyrocopter plea bargains, no-fly waivers, and minimal border and port security. Credibility is critical, as well as applying the maximum amount of force and security measures on potential Club-K entries into the country. Enforcing high standards and taking the appropriate amount of time to inspect all inbound cargo will mitigate vulnerabilities and subsequent future disasters.

Conclusion

In closing, NORAD has proven to evolve based on the National Security Strategy goals and threat assessment (i.e. symmetric, counterdrug, and asymmetric). The latter is an area that intelligence agencies thwarted once, but assert will continue until vulnerabilities are no longer exploitable. NORAD stands ready to defend the sovereignty of the United States (U.S.) 24/7, but must effectively integrate with the other active partners (i.e. government and civilian sector), by mitigating communication, security classifications, and jurisdiction barriers.

Constitutionally, the top priority of the U.S. government is to protect its citizens and infrastructure. However, the Global War on Terrorism continues and adversaries adapt and develop new tactics to target the U.S. homeland, which intelligence organizations deem will continue via the emerging low RCS technology capabilities. Based on research findings, this paper provides seven recommendations for consideration to possibly remedy an asymmetric attack, stemming from modifying deterrence, detection, and defeating methods. Specifically, it deems enforcing policy and removing constraints, ensuring detection capabilities via shared and separated sensors, and allocating sufficient alert assets to defeat any aerial threat as paramount.

Regardless, NORAD has the responsibility to deter, detect, and defeat all aerial threats entering its AOR, thus should not filter its sensors for the sake of other government agencies (i.e. FAA) to serve a secondary mission. If unable, then additional sensor or new technologies should cover vulnerable gaps. Additionally, the U.S. policies and intelligence organizations are key factors that will facilitate and inhibit counterterrorism efforts and the NORAD mission. Joint interoperability throughout federal, state, and local actors is necessary for legal authority and to fulfill the basic doctrine principle that emphasizes unity of effort. In modern times, NORAD cannot, and should not, act alone, despite being ultimately accountable for the defense of the homeland against low RCS technologies or any other innovative airborne threat concerning national security.

Lastly, a key finding in the 9/11 Commission Report was that "the institution charged with protecting our borders, civil aviation, and national security did not understand how grave the threat could be, and did not adjust their policies, plans, and practices to deter or defeat it." As a result, NORAD must not repeat history by failing to adapt its procedures to deter, detect, and defeat the new low RCS threat. It is clear that NORAD vulnerabilities exist, but one unknown remains. Will terrorists strike first or will NORAD makes changes to adequately defend the homeland against the emerging threat of a low RCS technology attack? This paper hopefully prompts further study and the government agencies responsible for homeland defense to take appropriate action.

APPENDIX
ABBREVIATIONS AND ACRONYMS

ADS:	air defense sector
AOR:	area of responsibility
ARS:	airport surveillance radar
ARSR:	air route surveillance radar
ASD (HD & ASA):	Assistant Secretary of Defense (Homeland Defense and Americas' Security Affairs)
AT:	anitterrorism
AWACS:	Airborne Warning and Control System
BMEWS:	Ballistic Missile Early Warning System
C2:	command and control
CBRNE:	chemical, biological, radiological, nuclear, and high-yield explosives
CDRNORAD:	Commander, North American Aerospace Defense Command
CIA:	Central Intelligence Agency
CJCS:	Chairman of the Joint Chiefs of Staff
CM:	cruise missile
COCOM:	combatant command (command authority)
COG:	center of gravity
COMINT:	communications intelligence
CONUS:	continental United States
CT:	counterterrorism
dB:	decibel
DCA:	Ronald Reagan Washington National Airport
DEFCON:	defense condition
DEN:	Domestic Events Network
DEW Line:	Distant Early Warning Line
DHS:	Department of Homeland Security
DNI:	Director of National Intelligence
DOD:	Department of Defense
DODD:	Department of Defense directive
DSCA:	defense support of civil authorities
DRSN:	Defense Red Switch Network
ELINT:	electronic intelligence
F2T2EA:	find, fix, track, target, engage, and assess (kill chain)
FAA:	Federal Aviation Administration
FBI:	Federal Bureau of Investigation
FEMA:	Federal Emergency Management Agency
FRZ:	flight restriction zone
GEOINT:	geospatial intelligence
GWOT:	Global War on Terror
HD:	homeland defense
HS:	homeland security

HUMINT:	human intelligence
IC:	intelligence community
ICAO:	International Civil Aviation Organization
ICBM:	intercontinental ballistic missile
IOP:	instruments of power
IPB:	intelligence preparation of the battlefield
ISR:	intelligence, surveillance, and reconnaissance
JIPOE:	joint intelligence preparation of the operational environment
JLENS:	Joint Land-Attack Cruise Missile Defense Elevated Netted Sensor System
JWICS:	Joint Worldwide Intelligence Communication System
LRDT:	long range detection team
m$^{2:}$	square meter
MASINT:	measurement and signature intelligence
NCR:	National Capital Region
NCR-IADS:	National Capital Region Integrated Air Defense System
NCTC:	National Counterterrorism Center
NMS:	national military strategy
NORAD:	North American Aerospace Defense Command
NOTAM:	Notice to Airmen
NSS:	national security strategy
NSSE:	national special security event
OPCON:	operational control
OSD:	Office of the Secretary of Defense
OSINT:	open-source intelligence
OTH-B:	over-the-horizon-backscatter
PAVE PAWS:	Perimeter Acquisition Vehicle Entry Phased Array Warning System
PCA:	Posse Comitatus Act
RCS:	radar cross-section
ROE:	rules of engagement
RPAS:	remotely piloted aircraft system
SAC:	Strategic Air Command
SIGINT:	signals intelligence
SLCM:	sea-launched cruise missile
SROE:	standing rules of engagement
TARS:	Tethered Aerostat Radar System
TECHINT:	technical intelligence
UCP:	Unified Command Plan
USCG:	United States Coast Guard
USNORTHCOM:	United States Northern Command
USSS:	United States Secret Service
VEO:	violent extremist organization
VFR:	visual flight rules

NOTES

1. *National Security Strategy*: Obama, 2015, 7.

2. Ibid., 2.

3. Steven Brusk and Ralph Ellis, "Russian Planes Intercepted Near U.S., Canadian Airspace," *CNN*, 13 November 2014, http://www.cnn.com/2014/09/19/us/russian-plane-incidents/ (accessed 29 February 2016).

4. "September 11th Fast Facts," *CNN*, 7 September 2015, http://www.cnn.com/2013/07/27/us/september-11-anniversary-fast-facts/ (accessed 29 February 2016).

5. House, *Gyrocopter Incident*, 2015.

6. Eugene Miasnikow, "Threat of Terrorism Using Unmanned Aerial Vehicles: Technical Aspects", *Open Sources Information*, June 2004, http://opensourcesinfo.org/threat-of-terrorism-using-unmanned-aerial-vehicles-technical-aspects/ (accessed 29 February 2016).

7. "Massachusetts Man Charged with Plotting Attack on Pentagon and U.S. Capitol," *FBI*, https://www.fbi.gov/boston/press-releases/2011/massachusetts-man-charged-with-plotting-attack-on-pentagon-and-u.s.-capitol-and-attempting-to-provide-material-support-to-a-foreign-terrorist-organization (accessed 29 February 2016).

8. *A Brief History of NORAD*, http://www.norad.mil/Portals/29/Documents/History/A%20Brief%20History-%20of%20NORAD.pdf (accessed 29 February 2016).

9. NORAD radar detection system, 1960. http://ed-thelen.org/72digest_f005.gif (accessed 29 February 2016).

10. Federation of American Scientists, "Strategic Air Defense," http://fas.org/nuke/guide/usa/airdef/-overview.htm (accessed 29 February 2016).

11. NORAD radar detection system, 1960. http://ed-thelen.org/72digest_f005.gif (accessed 29 February 2016).

12. David F. Winkler, "Searching the Skies: The Legacy of the United States Cold War Defense Radar Program," http://fas.org/nuke/guide/usa/airdef/searching_the_skies.htm (accessed 29 February 2016).

13. Federation of American Scientists, "Strategic Air Defense," http://fas.org/nuke/guide/usa/airdef/overview.htm (accessed 29 February 2016).

14. U.S. Department of State Office of the Historian, *The Cuban Missile Crisis*, *October 1962*, https://history.state.gov/milestones/1961-1968/cuban-missile-crisis (accessed 29 February 2016).

15. Christopher Bolkcom, "Homeland Security: Defending U.S. Airspace." https://www.fas.org/sgp-/crs/homesec/RS21394.pdf (accessed 29 February 2016).

16. National Commission on Terrorist Attacks Upon the United States, "The 9/11 Commission Report," http://www.9-11commission.gov/report/ (accessed 29 February 2016).

17. Ibid.

18. *9/11 Commission Report*, https://www.gpo.gov/fdsys/pkg/GPO-911REPORT/pdf/GPO-911REPORT.pdf (accessed 29 February 2016), 16.

19. Jim Garamone, "Short History of Homeland Defense," *American Forces Press Service*, 25 October 2001, http://www.au.af.mil/au/awc/awcgate/dod/hist-hld.htm (accessed 29 February 2016).

20. Rutger University Law Review, http://www.rutgerslawreview.com/category/special-section/page/2/ (accessed 29 February 16).

21. Testimony, *FBI*, https://www.fbi.gov/news/testimony/terrorism-are-americas-water-resources-andenvironment-at-risk (accessed 29 February 2016).

22. Eastern Air Defense Sector Tour Briefing, 2016.

23. William Knight, "Homeland Security: Roles and Missions for United States Northern Command," CRS Report for Congress, 3 June 2008, https://www.fas.org/sgp/crs/homesec/RL34342.pdf (accessed 29 February 2016).

24. Ibid.

25. Ibid.

26. Eastern Air Defense Sector Tour Briefing, 2016.

27. House, *Gyrocopter Incident*, 2015.

28. Akinbola E. Akinwumi, *International Journal of Baudrillard Studies*, Volume 3, Number 1, January 2006, http://www2.ubishops.ca/baudrillardstudies/vol3_1/akinbola.htm (accessed 29 February 2016).

29. Amy Zalman, "History of Terrorism," 31 July 2015, http://terrorism.about.com/od/whatisterroris1/p/-Terrorism.htm (accessed 29 February 2016).

30. "Fort Hood: An Act of Terrorism or an Act of Mass Murder?" https://community.aarp.org/t5/-Politics-Current-Events/Fort-Hood-An-Act-of-Terrorism-or-an-Act-of-Mass-Murder/m-p/991501 (accessed 29 February 2016).

NOTES

31. “A Brief History of the FAA,” https://www.faa.gov/about/history/brief_history/ (accessed 29 February 2016).

32. Samuel Francis, *The Omnibus Antiterrorism Act*, http://www.heritage.org/research/-reports/1978/09/the-omnibus-antiterrorism-act (accessed 29 February 2016).

33. Presidential Decision Directives (PDD) 39, *U.S. Policy on Counterterrorism*. 10.

34. Rory Brown, “Shooting Down Civilian Aircraft: Illegal, Immoral and Just Plane Stupid,” http://www-.sqdi.org/-wp-content/uploads/20.1_brown.pdf (accessed 29 February 2016), 60.

35. Convention on International Civil Aviation [Article 3 bis], https://www.mcgill.ca/iasl/files/iasl/montreal-1984.pdf (accessed 29 February 2016).

36. Ibid.

37. Loch K. Johnson, *Strategic Intelligence*, 4.

38. Ibid., 4.

39. Ibid., 4.

40. “MASINT: Intelligence of the Future,” https://www.dsta.gov.sg/docs/publications-documents/dh2007-_chapter_10.pdf?sfvrsn=2 (accessed 29 February), 4.

41. “Geospatial Intelligence (GEOINT),” http://www.defence.gov.au/AGO/geoint.htm (accessed 29 February 2016).

42. “U.S. National Intelligence Overview 2013,” http://www.slideshare.net/RobSentseBc/us-nationalintell-igence-overview-2013 (accessed 29 February 2016).

43. Ibid.

44. Ibid.

45. JP 3-27, III-3.

46. “U.S. National Intelligence Overview 2013.”

47. *Military Ground Control Centers, United States*, http://what-when-how.com/space-science-and-technology-/-military-ground-control-centers-united-states/ (accessed 29 February 2016).

48. World Affairs Council, *William Gortney: A Commander’s Perspective on Securing America*,25 January 2016, https://www.youtube.com/watch?v=_SR2Pml14zs (accessed 29 February 2016).

49. JP 1-02, 67.

50. Adam, Lowther, “Thinking about Deterrence,” http://www.au.af.mil/au/aupress/digital/pdf/book/b_0133-_lowther_thinking_about_deterrence.pdf (accessed 29 February 2016), 201.

51. Ibid., 205.

52. JP 3-27, I-1.

53. “What Really Causes Terrorism? It’s Not Your Freedom,” http://thinkbynumbers.org/terrorism/suicide-terrorism-statistics/ (accessed 29 February 2016).

54. “Budget Cuts Impact 24-Hour Alert Status of 148th Fighter Wing,” *KBJR News 1*, 26 August 2013, http://www-.northlandsnewscenter.com/news/local/Budget-Cuts-Impact-24-Hour-Alert-Status-of-148th-Fighter-Wing-221233831.html (accessed 29 February 2016).

55. JP 3-12, *Cyberspace Operations*, 5 February 2013, I-4.

56. “North American Aerospace Defense Command,” *Wikiwand*, http://www.wikiwand.com/en/North-_American_Aerospace_Defense_Command (accessed 29 February 2016).

57. Adam, Lowther, “Thinking about Deterrence,” http://www.au.af.mil/au/aupress/digital/pdf/book/b_0133-_lowther_thinking_about_deterrence.pdf (accessed 29 February 2016), 199.

58. Ibid., 199.

59. Ibid., 199.

60. FAA, “NOTAM Number: FDC 6/2069,” 9 February 2016, http://www.faa.gov/news/updates/media/sUAS-_SFRA_FDC_6_2069_A0037_16.pdf (accessed 29 February 2016).

61. CRS Report for Congress, “Homeland Security: Protecting Airspace in the National Capital Region,” 1 September 2005, https://www.fas.org/sgp/crs/homesec/RS22234.pdf (accessed 29 February 2016).

62. Ibid.

63. Adam, Lowther, “Thinking about Deterrence,” http://www.au.af.mil/au/aupress/digital/pdf/book/b_0133-_lowther_thinking_about_deterrence.pdf (accessed 29 February 2016), 8.

64. JP 3-01, *Countering Air and Missile Threats*, 23 March 2012, I-7.

NOTES

65. C. Trueman, "The V1," 21 April 2015, http://www.historylearningsite.co.uk/world-war-two/world-war-two-in-western-europe/the-v-revenge-weapons/the-v1/ (accessed 29 February 2016).

66. Federal Aviation Administration, "FAA Data." https://aspm.faa.gov/opsnet/sys/opnet-server-s.asp (accessed 29 February 2016).

67. House, *Gyrocopter Incident*, 2015.

68. JP 3-01, V-12.

69. Loren Thompson, "Modernizing the Air Force's Electronic Aircraft Fleet," http://www.nationaldefense-magazine.org/blog/Documents/Lexingnton_ElectronicAircraftFleet.pdf (accessed 29 February 2016).

70. House, *Gyrocopter Incident*, 2015.

71. Ibid.

72. "Radar Cross Section," *Global Security.org*, http://www.globalsecurity.org/military/world/stealth-aircraft-rcs.htm (accessed 29 February 2016).

73. *9/11 Commission Report*, 20.

74. Kyle Noth and Daniel Luke, "Modeling and Simulation of Ground Based Radar Surveillance Solutions for Unmanned Aircraft Systems," http://enu.kz/repository/2011/AIAA-2011-6375.pdf (accessed 29 February 2016).

75. JP 3-27, ix.

76. JP 3-30, *Command and Control of Joint Air Operations*, 10 February 2014, II-2.

77. Ibid., II-25.

78. "Brief History of the FAA," https://www.faa.gov/about/history/brief_history/ (accessed 29 February 2016).

79. U.S. Department of Transportation, "Special Operations," 3 April 2014, http://www.slideshare.net/Vallee-17/faa-special-operations (accessed 29 February 2016).

80. Ibid.

81. FAA, "NOTAM Number: FDC 0/8326," 18 November 2010, http://tfr.faa.gov/save_pages/detail_0_8326-.html (accessed 29 February 2016).

82. JP 3-27, Homeland Defense, 12 July 2007, III-5.

83. *National Security Strategy*: Bush, 2015, 27.

84. Douglas Feith, U.S. Department of State, *Operation Enduring Freedom: 1 Year Later*, http://2002-2009-fpc.state.gov/14209.htm (accessed 29 February 2016).

85. *National Strategy for Combating Terrorism*, http://2001-2009.state.gov/s/ct/rls/wh/71803.htm (accessed 29 February 2016).

86. *National Strategy for Counterterrorism*, June 2001, https://www.whitehouse.gov/sites/default/files/-counter-terrorism_strategy.pdf (accessed 29 February 2016).

87. *NMS*, June 2015, http://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy-.pdf (accessed 29 February 2016).

88. Ibid., 1.

89. Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 15 November 2015, 245.

90. Ibid., 14.

91. Ibid., 54.3-08.

92. Ibid., 39.

93. Ibid., 106.

94. JP 3-08, *Interorganizational Coordination During Joint Operations*, 24 June 2011, II-22.

95. JP 3-27, *Homeland Defense*, 29 July 2013, A-2.

96. Ibid., II-3.

97. JP 2-01, *Joint and National Intelligence Support to Military Operations*, 5 January 2012, II-30.

98. JP 3-26, *Counterterrorism*, 24 October 2014, II-20.

99. Ibid., I-2.

100. Ibid., I-1.

101. Ibid., I-1.

102. Ibid., I-1.

NOTES

103. Ibid., I-1.

104. FBI,*Testimony* 24 July 2002, https://www.fbi.gov/news/testimony/intelligence-and-counterterrorism (accessed 29 February 2016).

105. Micael Spak and Donald Sparks, “Posse Comitatus Act (1878),” *Encyclopedia.com*, http://www.encyclopedia.-com/topic/Posse_Comitatus_Act.aspx (accessed 29 February 2016).

106. JP 3-27, viii.

107. Eric Larson and John Peters, “Preparing the U.S. Army for Homeland Security: Concepts, Issues, and Options.” *RAND Corporation*, http://www.rand.org/pubs/monograph_reports/MR1251.html (accessed 29 February 2016).

108. Ibid

109. JP 3-01, III-1.

110. JP 2-01, V-3.

111. House, *Gyrocopter Incident*, 2015.

112. JP 3-27, I-6.

113. Mario Carrillo and Jean Lumley, NSSE Briefing, 4 March 2008, http://rnc08report.org/engine/uploads/1/Day-2-Breakout-2-NSSE-Carillo-Lowry-Lumley.pdf (accessed 29 February 2016).

114. House, *Gyrocopter Incident*, 2015.

115. Ibid.

116. Club-K Container Missile System 2013, Youtube, 8 min, 4 sec., https://www.youtube.com/watch?v=mb-UU-_9bOcnM (accessed 29 February 2013).

117. Marhalim Abas, , “Club-K Missile System for Malaysia?” *Malaysian Defence*, August 2013, http://www.malaysiandefence.com/?=3586 (accessed 29 February 2016).

BIBLIOGRAPHY

"9/11 Commission Report." https://www.gpo.gov/fdsys/pkg/GPO-911REPORT/pdf/GPO-911REPORT.pdf (accessed 29 February 2016).

"A Brief History of NORAD." http://www.norad.mil/Portals/29/Documents/History/A%20-Brief%20History%20of%20NORAD.pdf (accessed 29 February 2016).

Akinwumi Akinbola E. *International Journal of Baudrillard Studies*, Volume 3, Number 1, January 2006, http://www2.ubishops.ca/baudrillardstudies/vol3_1/akinbola.htm (accessed 29 February 2016).

Benjamin, Daniel. "National Strategy for Counterterrorism." 20 July 2011. http://www.state.gov/j/ct/rls/rm/2011/169022.htm (accessed 29 February 2016).

Bolkcom, Christopher. "Homeland Security: Defending U.S. Airspace." 6 June 2006. https://www.fas.org/sgp-/crs/homesec/RS21394.pdf (accessed 29 February 2016).

Brown, Rory S. "Shooting Down Civilian Aircraft: Illegal, Immoral and Just Plane Stupid." http://www.sqdi.org/wp-content/uploads/20.1_brown.pdf (accessed 29 February 2016).

Brusk, Steve, and Ralph Ellis. "Russian Planes Intercepted Near U.S. Canadian Airspace." *CNN*, 13 November 2014. http://www.cnn.com/2014/09/19/us/russian-plane-incidents/ (accessed 29 February 2016).

"Budget Cuts Impact 24-Hour Alert Status of 148th Fighter Wing," *KBJR News 1*, 26 August 2013, http://www-.northlandsnewscenter.com/news/local/Budget-Cuts-Impact-24-Hour-Alert-Status-of-148th-Fighter-Wing-221233831.html (accessed 29 February 2016).

Carrillo, Mario, and Jean Lumley. "NSSE Briefing," 4 March 2008, http://rnc08report.org/-engine-/uploads/1/Day-2-Breakout-2-NSSE-Carillo-Lowry-Lumley.pdf (accessed 29 February 2016).

Convention on International Civil Aviation. *Chicago Convention: Article 3BIS*. 10 May 1984.

Cornell University Law School. 10 U.S. Code § 153 - Chairman: functions, https://www.law-.cornell.edu/uscode-/text/10/153 (accessed 29 February 2016).

CRS Report for Congress. "Homeland Security: Protecting Airspace in the National Capital Region." 1 September 2005, https://www.fas.org/sgp/crs/homesec/RS22234.pdf (accessed 29 February 2016).

CSPAN, *House Oversight and Government Reform Committee Hearing - Gyrocopter Incident.*, 2015; 131 min., 10 sec. http://www.c-span.org/video/?325628-1/hearing-washington-dc-airspace-security# (accessed 29 February 2016).

BIBLIOGRAPHY

Department of Defense (DOD) Directive 2000.12. DOD Combating Terrorism Program, 15 September 1996.

FAA, “NOTAM Number: FDC 6/2069,” 9 February 2016, http://www.faa.gov/news/updates/-media/sUAS-_SFRA_FDC_6_2069_A0037_16.pdf (accessed 29 February 2016).

Federal Aviation Administration. “Brief History of the FAA,” https://www.faa.gov/about-/history/brief_history/ (accessed 29 February 2016).

Federal Aviation Administration. “FAA Data.” https://aspm.faa.gov/opsnet/sys/opnet-server-s.asp (accessed 29 February 2016).

Federal Aviation Administration. “NOTAM Number: FDC 0/8326,” 18 November 2010, http://tfr.faa.gov/save_pages/detail_0_8326.html (accessed 29 February 2016).

Federation of American Scientists. “NORAD at 40: Historical Overview.” http://fas.org/nuke/-guide/usa/airdef-/overview.htm.

Federation of American Scientists. “Strategic Air Defense.” http://fas.org/nuke/guide/usa/airdef-/overview.htm.

Federation of American Scientist, “Terrorism and the Military’s Role in Domestic Crisis Management,” http://fas.org/irp/crs/RL30938.pdf (accessed 29 February 2016).

Federal Bureau of Investigations (FBI). “Massachusetts Man Charged with Plotting Attack on Pentagon and U.S. Capitol,” 28 September 2011. https://www.fbi.gov/boston-/press-releases/2011/massachusetts-man-charged-with-plotting-attack-on-pentagon-and-u.s.-capitol-and-attempting-to-provide-material-support-to-a-foreign-terrorist-organization (accessed 29 February 2016).

Feith, Douglas J. “Operation Enduring Freedom: 1 Year Later.” 8 October 2002. http://2002-2009-fpc.state.gov/14209.htm (accessed 29 February 2016).

Francis, Samuel. “The Omnibus Antiterrorism Act.” http://www.heritage.org/research/reports/-1978/09/the-omnibus-antiterrorism-act (accessed 29 February 2016).

Garamone, Jim. “A Short History of Homeland Defense.” 25 October 2001. http://www.au.af.-mil/au/awc/awcgate/dod/hist-hld.htm (accessed 29 February 2016).

Gortney, William Adm. “Statements for the House Armed Services Committee, Strategic Forces Subcommittee.” 19 March 2015.

BIBLIOGRAPHY

Joint Publication (JP) 1-02. *Department of Defense Dictionary of Military and Associated Terms*, 15 November 2015.

Joint Publication (JP) 2-01. *Joint and National Intelligence Support to Military Operations*, 5 January 2012.

Joint Publication (JP) 3-01. *Countering Air and Missile Threats*, 23 March 2012.

Joint Publication (JP) 3-08. *Interagency Coordination During Joint Operations*, 24 June 2011.

Joint Publication (JP) 3-12. *Cyberspace Operations*, 5 February 2013.

Joint Publication (JP) 3-26. *Counterterrorism*, 24 October 2014.

Joint Publication (JP) 3-27. *Homeland Defense*, 12 July 2007.

Joint Publication (JP) 3-27. *Homeland Defense*, 29 July 2013.

Joint Publication (JP) 3-30. *Command and Control of Joint Air Operations*, 10 February 2014.

Knight, William. "Homeland Security: Roles and Missions for USNORTHCOM." https://www.fas.org/sgp/crs/homesec/RL34342.pdf (accessed 29 February 2016).

Larson, Eric and John Peters. "Preparing the U.S. Army for Homeland Security: Concepts, Issues, and Options." http://www.rand.org/pubs/monograph_reports/MR1251.html (accessed 29 February 2016).

Lowther, Adam. "Thinking about Deterrrence." http://www.au.af.mil/au/aupress/digital/pdf/book/b_0133_lowther_thinking_about_deterrence.pdf (accessed 29 Feburary 2016).

McCraw, Steven. FBI Testimony. 24 July 2003. https://www.fbi.gov/news/testimony/intelligence-and-counterterrorism (accessed 29 February 2016).

Miasnikov, Eugene. "Threat of Terrorism Using Unmanned Aerial Vehicles: Technical Aspects." http://opensourcesinfo.org/threat-of-terrorism-using-unmanned-aerial-vehicles-technical-aspects/ (accessed 29 February 2016).

Military Ground Control Centers, United States. http://what-when-how.com/space-science-and-technology/-military-ground-control-centers-united-states/ (accessed 29 February 2016).

National Commission on Terrorist Attack Upon the United States, "The 9/11 Commission Report." 2002. http://www.9-11commission.gov/report/ (accessed 29 February 2016).

BIBLIOGRAPHY

National Military Strategy (NMS), June 2015.

National Security Strategy (NSS), February 2002.

National Security Strategy (NSS), February 2015.

National Strategy for Combating Terrorism, September 2006.

North American Aerospace Defense Command. http://www.wikiwand.com/en/North-_American_Aerospace_Defense_Command (accessed 29 February 2016).

Noth, Kyle and Daniel Luke. *Modeling and Simulation of Ground Based Radar Surveillance Solutions for Unmanned Aircraft Systems*. http://enu.kz/repository/2011/AIAA-2011-6375.pdf (accessed 29 February 2016).

Poulsen, Kevin. "Why the US Government is Terrified of Hobbyist Drones." 5 February 2015. http://www.wired.com/2015/02/white-house-drone/ (accessed 29 February 2016).

Presidential Decision Directives (PDD) 39, *U.S. Policy on Counterterrorism*, 21 June 1995.

Rutgers University Law Review. "United 175." http://www.rutgerslawreview.com/category-/special-section/page/2/ (accessed 29 February 2016).

"September 11th Fast Facts." *CNN.com*, 7 September 2015. http://www.cnn.com/2013/07/27/-us/september-11-anniversary-fast-facts/ (accessed 29 February 2016).

Shaw, Jonathan E. "*The Role of Religion in National Security Policy Since September 11, 2001,"* U.S. Army War College, Carlisle Papers, 2011,   http://www.strategic-studiesinstitute.army.mil/pdffiles/PUB1044.pdf (accessed 29 February 2016).

Spak, Michael I., and Donald F. Sparks. "Posse Comitatus Act (1878). Encyclopedia.com. http://www.encyclopedia.com/topic/Posse_Comitatus_Act.aspx (accessed 29 February 2016).

Trueman, C. "The V1." 21 April 2015. http://www.historylearningsite.co.uk/world-war-two/world-war-two-in-western-europe/the-v-revenge-weapons/the-v1/ (accessed 29 February 2016).

Trimble, Stephen. "USAF Grapples With Air Sovereignty Alert Mission a Decade After 9/11", *Flightglobal*, 6 September 2011. https://www.flightglobal.com/news/-articles/usaf-grapples-with-air-sovereignty-alert-mission-a-d-361387/ (accessed 29 February 2016).

BIBLIOGRAPHY

Thompson, Loren. “Modernizing the Air Force’s Electronic Aircraft Fleet,” http://www.national-defensemagazine.org/blog/Documents/Lexingnton_ElectronicAircraftFleet.pdf (accessed 29 February 2016).

US Department of State. “The Cuban Missile Crisis, October 1962.” https://history.state.gov/-milestones/1961-1968/cuban-missile-crisis.

U.S. Department of Transportation. “Special Operations,” 3 April 2014. http://www.slideshare-.net/Vallee17/faa-special-operations (accessed 29 February 2016).

“U.S. National Intelligence Overview 2013.” http://www.slideshare.net/RobSentseBc/us-national-intelligence-overview-2013 (accessed 29 February 2016).

“What Really Causes Terrorism? It’s Not Your Freedom.” http://thinkbynumbers.org/terrorism-/suicide-terrorism-statistics/ (accessed 29 February 2016).

Winkler, David F. “Searching the Skies: The Legacy of the United States Cold War Defense Radar Program,” June 1997. http://fas.org/nuke/guide/usa/airdef/searching_the_skies.htm (accessed 29 February 2016).

World Affairs Coucil, *William Gortney: A Commander’s Perspective on Securing America,* 25 January 2016, 63 min., 23 sec. https://www.youtube.com/watch?v=_SR2Pml14zs (accessed 29 February 2016).

Zalman, Amy. “The History of Terrorism.” 31 July 2015. http://terrorism.about.com/od/whatis-terroris1/p/Terrorism.htm (accessed 29 February 2016).